ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

RECEIVED
CENTRAL FAX CENTER
APR 17 2006

FAX COVER SHEET

Date:	April 17, 2006	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals & Interferences		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P040/01.254.01 **App. No: 10/006,549**

Total Number of Pages Being Transmitted, Including Cover Sheet: 35

Message:

Please deliver to the Board of Patent Appeals and Interferences.

Thank you,

Kevin J. Zilka

☑ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

April 17, 2006

Practitioner's Docket No. NAIIP040/01.254.01

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Michael C. Pak et al.

Application No.: 10/006,549 Group No.: 2132
Filed: November 30, 2001 Examiner: Perungavoor, V.
For: DELAYED-DELIVERY QUARANTINING OF NETWORK COMMUNICATIONS HAVING SUSPICIOUS CONTENTS

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on February 15, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. ' ' 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is *mandatory;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*

_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ _ facsimile transmitted to the Patent and Trademark Office, (571) 273 -8300.

Date: 4/17/2006

Signature

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$500.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $500.00 to Deposit Account No. 50-1351 (Order No. NAI1P040).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P040).

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Pak et al.	Group Art Unit: 2132
Application No. 10/006,549	Examiner: Perungavoor, V.
Filed: November 30, 2001	Date: April 17, 2006
For: DELAYED-DELIVERY QUARANTINING OF NETWORK COMMUNICATIONS HAVING SUSPICIOUS CONTENTS	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on February 15, 2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI ISSUES
VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-6, 8-15, 17, 18 and 20-31

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-6, 8-15, 17, 18 and 20-31
3. Claims allowed: None
4. Claims rejected: 1-6, 8-15, 17, 18 and 20-31
5. Claims cancelled: 7, 16 and 19

C. CLAIMS ON APPEAL

The claims on appeal are: 1-6, 8-15, 17, 18 and 20-31

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claims 1, 9 and 10, as shown in Figure 3, a system, method and computer program product are provided for network-based scanning for potentially malicious content, including monitoring network communications over a network (e.g. item 302 of Figure 3). In use, potentially malicious content in the network communications is identified (e.g. item 308 of Figure 3). The potentially malicious content of the network communications is then quarantined (e.g. item 310 of Figure 3), and a pattern is executed for testing the potentially malicious content network communications for malicious code. In addition, the network communications are conditionally delivered over the network based on the testing (e.g. item 318 of Figure 3). Furthermore, the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content. See page 10, lines 6-12; page 10, line 25-page 11, line 2; page 12, lines 1-5; and page 13, line 5-page 14, line 28, for example.

With respect to a summary of Claim 11, the above summary is incorporated at least in part. Additionally, the network communications are delivered over the network after a predetermined delay (e.g. item 324 of Figure 3). See page 14, lines 11-15, for example.

With respect to a summary of Claim 17, the summary with respect to Claims 1, 9 and 10 is incorporated at least in part. Further, the network communications are delivered from the quarantine over the network in response to a request from a user (e.g. item 326 of Figure 3). It is also determined whether the user is authorized, and the network communications are delivered only if the user is determined to be authorized (e.g. item 328 of Figure 3). See page 14, lines 17-22, for example.

With respect to a summary of Claim 23, as shown in Figures 3 and 4, a method is provided for network-based scanning for potentially malicious content, including monitoring incoming and outgoing network communications over a network at a gateway (e.g. item 302 of Figure 3 . In use, the network communications are scanned for known malicious content (e.g. item 404 of Figure 4) and potentially malicious content is identified in the network communications (e.g.

item 406 of Figure 4). In one aspect, content is identified as potentially malicious when a number of identical instances of the content in the network communications passing through the network for a given period of time is greater than a predetermined value. Such network communications include electronic mail messages, where an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line passing through the network for a given period of time is greater than a predetermined value. In addition, the potentially malicious content of the network communications is quarantined (e.g. item 310 of Figure 3). The network communications are then delivered over the network upon occurrence of the first of (1) the potentially malicious content is scanned with a malicious code detection file received after the potentially malicious content is received (e.g. items 314 and 316 of Figure 3), (2) a user request is received (e.g. item 326 of Figure 3), and (3) upon passage of a predetermined amount of time (e.g. item 324 of Figure 3). Still yet, an intended recipient of the potentially malicious content is notified that the potentially malicious content has been quarantined, and a sender of the potentially malicious content is notified that the potentially malicious content has been quarantined. In addition, the potentially malicious content is cleaned if malicious code is found, which is disabling of malicious code (e.g. item 408 of Figure 4). See page 10, lines 6-19; page 11, line 8-page 12, line 5; page 12, lines 14-28; page 13, line 5-19; and page 14, lines 11-20, for example.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-2, 5-6, 812, 14-15, 17-19, 21-22, 24 and 26-31 under 35 U.S.C. 102(b) as being anticipated by Hitachi, Ltd (EP 0893769 A1).

Issue # 2: The Examiner has rejected Claims 3, 4, 13, 20 and 23 under 35 U.S.C. 103(a) as being unpatentable over Hitachi, Ltd (EP 0893769 A1), in view of Arnold et al. (U.S. Patent No. 5,440,723).

Issue # 3: The Examiner has rejected Claim 25 under 35 U.S.C. 103(a) as being unpatentable over Hitachi, Ltd (EP 0893769 A1), in view of Arnold et al. (U.S. Patent No. 5,440,723).

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-2, 5-6, 8-12, 14-15, 17-18, 21-22, 24 and 26-31 under 35 U.S.C. 102(b) as being anticipated by Hitachi, Ltd (EP 0893769 A1).

Group #1: Claims 1-2, 5, 9-12, 14, 17, 21, 24 and 26

With respect to independent Claims 1, 9-11 and 17, the Examiner has relied on Col. 5, lines 21-39; Col., 8, lines 48-57 and steps 801-823 in Figure 8 of Hitachi to make a prior art showing of appellant's claimed technique "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content."

In the latest Office Action dated 12/14/2005, the Examiner has argued that Hitachi discloses "the malicious detection file received after the malicious content see Fig. 8 item 805 and Col 13 Ln 52-Col 14 Ln 19, where the procedure is determined after the quarantine has taken place, i.e. see decision box "data infections?" and that the "Hitachi quarantine(Fig.8 step 804)...takes place before the scanning(Fig. 8 step 805)."

Appellant respectfully asserts that the above excerpt from Hitachi does not even suggest that "the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content," as claimed. In particular, appellant points out that the Examiner references operation 805 in Figure 8 and Col. 13, lines 52-Col. 14, lines 19 to meet such claim language. Appellant emphasizes, however, that operation 805 in Figure 8 only shows "determin[ing a] download procedure of [the] file" after "transfer[ing] and quarantin[ing the] file suspected for infection" in operation 804. Thus, Hitachi excerpt teaches that only the infected file is downloaded

after such infected file is quarantined, and not that "a malicious code detection file [is] received after the potentially malicious content," as claimed by appellant (emphasis added).

To further emphasize such distinction, appellant points out that Hitachi expressly discloses that "[i]n step 805, the security agent 651 again notifies to the virus buster 650 in advance a procedure of moving the file 613 transferred in step 803 onto the hard disk 612" where such file 613 is the "file 613 suspected for infection with a computer virus of a new type" (see Col. 13, lines 35-51). Clearly, Hitachi teaches that the same file is quarantined and then downloaded, which cannot meet appellant's claim language of a different entity, namely the "malicious code detection file" that is "received after the potentially malicious content," as specifically claimed by appellant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Hitachi reference, since Hitachi fails to at least suggest all of appellant's claim limitations, as noted above.

Group #2: Claims 6, 15 and 22

The Examiner has relied on Col. 7, lines 34-45 in Hitachi to make a prior art showing of appellant's claimed technique "wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value." In addition, the latest Office Action dated 12/14/2005, the Examiner has responded to appellant's arguments by stating that Arnold (U.S. Patent No. 5,440,723) "discloses the protection of a mass mailer, where the subject line is compared" in Col. 2, lines 14-25.

First, appellant notes that the Examiner has rejected Claims 6, 15 and 22 under 35 U.S.C. 102(b) as being anticipated by Hitachi (EP 08093769 A1), and has then relied on an excerpt from Arnold to meet appellant's claim language. Appellant respectfully asserts that such specific rejection is inappropriate.

Second, appellant respectfully asserts that Col. 2, lines 14-25 in Arnold merely discloses that "[w]hen a computer finds that it is infected with a virus, it sends a message to every computer that it has ever contacted or been contacted by, which in turn send messages to all of their contactees or contactors, etc." Thus, Arnold only teaches a situation where a single computer contacts its contacts and those contacts' contacts to inform them that such single computer is infected with a virus. Clearly, such disclosure in Arnold does not even suggest "a number of messages having an identical subject line," let alone where such number of messages "is greater than a predetermined value," in the manner specifically claimed by appellant (emphasis added).

Third, appellant respectfully asserts that Col. 7, lines 34-45 in Hitachi merely teaches open keys that are utilized to verify the validity of digital signatures. Simply nowhere in such excerpt is there any disclosure of messages, let alone in the specific manner claimed by appellant.

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #3: Claim 8

The Examiner has relied on Col. 9, lines 18-30 in Hitachi to make a prior art showing of appellant's claimed "cleaning the potentially malicious content if malicious code is found, which is disabling of malicious code." Appellant respectfully asserts that such excerpt only discloses "mov[ing the security software] to the lower-most position on the activation list" and "delet[ing] the software." Clearly, moving and deleting security software, where such software is used for security purposes, as disclosed in Hitachi (see Abstract), does not even suggest "cleaning the potentially malicious," as claimed by appellant.

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #4: Claim 18

The Examiner has relied on Col. 5, line 54-Col. 6, line 6 in Hitachi to make a prior art showing of appellant's claimed technique "wherein the user is an intended recipient of the quarantined network communications." Appellant respectfully asserts that such excerpt only teaches adding moving type security dedicated software to messages sent by computers, where the recipients of such messages execute the software added to the messages utilizing a fixed type security dedicated module. Clearly, such excerpt does not even suggest quarantined network communications, as claimed by appellant, since the message in Hitachi are being sent between computers.

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #5: Claim 27

The Examiner has relied on Figure 8, items 803-804 and Col. 7, line 46-Col. 8, line 26 in Hitachi to make a prior art showing of appellant's claimed technique "wherein when multiple recipients are to receive a copy of the potentially malicious content over the network, a single copy of the potentially malicious content is quarantined and each of the recipients is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients." In addition, the latest Office Action dated 12/14/2005, the Examiner has responded to appellant's arguments by stating that "Hitachi discloses the determination of quarantined file is not infected forwarding it to the recipients" in Col. 14, lines 5-19 and Figure 1, items 102-107.

First, appellant respectfully asserts that Col. 14, lines 5-19 in Hitachi only teaches that "[w]hen an injustice is detected...the virus buster 650 stores the file just transferred from a computer on the network to be separated from the file in which the illness is not detected for a predetermined

period of time." Clearly, storing files transferred from a computer, as in the Hitachi excerpt, does not meet appellant's specific claim language, namely "when multiple recipients are to receive a copy of the potentially malicious content over the network, a single copy of the potentially malicious content is quarantined" (emphasis added), as claimed. To emphasize, Hitachi teaches quarantining any transferred file, whereas appellant claims quarantining a single copy when multiple recipients are to receive a copy.

In addition, appellant notes that Hitachi fails to even suggest a situation where "multiple recipients are to receive a copy of the potentially malicious content over the network," as appellant claims, and therefore the Hitachi excerpt cannot meet appellant's claim language requiring that "each of the recipients is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients," as claimed.

Second, appellant respectfully asserts that items 804 and 805 of Figure 8 in Hitachi merely show quarantining a file and determining a download procedure for the file. Further, Col. 7, line 46-Col. 8, line 26 simply relates to data that is "communicated between the personal computer A 101 and the WWW server 102." Again, appellant notes that simply nowhere does the Hitachi excerpt teach a situation where "multiple recipients are to receive a copy of the potentially malicious content over the network," as appellant claims (emphasis added), and thus Hitachi cannot meet appellant's specific claim language.

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #6: Claim 28

The Examiner has again relied on Figure 8, items 803-804 and Col. 7, line 46-Col. 8, line 26 in Hitachi to make a prior art showing of appellant's claimed technique "wherein an intended recipient of the network communications is notified that the potentially malicious content is quarantined." Appellant again respectfully asserts that items 804 and 805 of Figure 8 in Hitachi merely show quarantining a file and determining a download procedure for the file and that Col.

7, line 46-Col. 8, line 26 simply relates to data that is "communicated between the personal computer A 101 and the WWW server 102." Simply nowhere in such excerpt in Hitachi is there even a suggestion of any sort of notification, let alone in the specific manner claimed by appellant.

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #7: Claim 29

The Examiner has relied on Figure 8, items 803-804; Col. 13, lines 44-51; and Col. 14, lines 5-19 to make a prior art showing of appellant's claimed technique "wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with the malicious code detection file received after the potentially malicious content and after the potentially malicious content is quarantined." Appellant respectfully asserts that simply nowhere in such excerpts is there any teaching the scanning "with the malicious code detection file received after the potentially malicious content and after the potentially malicious content is quarantined," as appellant claims (emphasis added).

Specifically, appellant notes that such excerpts teach "transfer[ing] the suspected file 613 to the file server 621" (emphasis added), and "stor[ing] the file just transferred...to be separated form the files in which the illness is not detected." Thus, Hitachi only teaches transferring the infected file for quarantining for the purpose of quarantining the infected file, and therefore does not even suggest a "malicious code detection file received after the potentially malicious content and after the potentially malicious content is quarantined," as appellant claims.

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #8: Claim 30

The Examiner has relied on Col. 13, lines 12-43 and Col. 12, lines 48-55 in Hitachi to make a prior art showing of appellant's claimed technique "wherein the malicious code detection file is created after the potentially malicious content is identified such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content." Appellant respectfully asserts that such excerpts only relate to the infected file, and do not even suggest any sort of "malicious code detection file," let alone where such detection file "is created after the potentially malicious content is identified such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content," as appellant specifically claims (emphasis added).

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Group #9: Claim 31

The Examiner has again relied on Col. 13, lines 12-43 and Col. 12, lines 48-55 in Hitachi to make a prior art showing of appellant's claimed technique "wherein the malicious code detection file is created after the potentially malicious content is received such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content." Again, appellant respectfully asserts that such excerpts only relate to the infected file, and do not even suggest any sort of "malicious code detection file," let alone where such detection file is "created after the potentially malicious content is received such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content," as specifically claimed by appellant (emphasis added).

Again, appellant respectfully asserts that Hitachi fails to teach all of appellant's claim limitations, for substantially the reasons noted above.

Issue # 2:

The Examiner has rejected Claims 3, 4, 13, 20 and 23 under 35 U.S.C. 103(a) as being unpatentable over Hitachi, Ltd (EP 0893769 A1), in view of Arnold et al. (U.S. Patent No. 5,440,723).

Group #1: Claim 3

The Examiner has relied on Col. 2, lines 14-25 in Arnold to make a prior art showing of appellant's claimed technique "wherein the malicious content includes a mass-mailer virus." Appellant respectfully asserts that such excerpt only discloses that "[w]hen a computer finds that it is infected with a virus, it sends messages to every computer that it has ever contacted or been contacted by, which in turn send messages to all of their contactees or contactors, etc." Clearly, a single computer sending messages to its contacts to inform those contacts that the single computer is infected, as in the Hitachi excerpt, does not even suggest a "mass-mailer virus," as appellant claims (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claims 4, 13 and 20

The Examiner has relied on Col. 9, lines 61-68 and Col. 10, lines 53-56 in Arnold to make a prior art showing of appellant's claimed technique "wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value." In addition, in the latest Office Action dated 12/14/2005, the Examiner has responded to appellant's arguments by stating that "Arnold discloses the malicious

content being determined when the number of instances of content greater than the predefined threshold see Fig. 7 item G and Col. 9 Ln 61-68 and Col 9 Ln 36-41, where [in] Hitachi the [statistical] measurements and probability is being used to determine if it is greater than a predetermined threshold."

First, appellant notes that simply nowhere in Hitachi is there any disclosure of probability, as the Examiner has argued. Thus, Hitachi can not meet appellant's specific claim language. Second, appellant respectfully asserts that the threshold disclosed in Arnold relates to "a [false-positive and false-rejection] probability threshold [that is] used for accepting or rejecting a candidate signature" (see Figure 7, items F and G; Col. 3, lines 41-43; and Col. 10, line 64-Col. 11, line 12). Clearly, determining a threshold for accepting signatures, as set forth in the Arnold excerpt, does not even suggest "content [that] is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value," as claimed by appellant (emphasis added).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claim 23

With respect to independent Claim 23, the Examiner has relied on Col. 7, lines 34-45 in Hitachi and Col. 9, lines 61-68 and Col. 10, lines 53-56 in Arnold to make a prior art showing of appellant's claimed technique "wherein content is identified as potentially malicious when a number of identical instances of the content in the network communications passing through the network for a given period of time is greater than a predetermined value; [and] wherein the network communications include electronic mail messages, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line passing through the network for a given period of time is greater than a predetermined value."

First, appellant respectfully asserts that Col. 7, lines 34-45 in Hitachi merely teaches open keys that are utilized to verify the validity of digital signatures. Simply nowhere in such excerpt is

there any disclosure of "content [that] is identified as potentially malicious when a number of identical instances of the content in the network communications passing through the network for a given period of time is greater than a predetermined value," as appellant claims. In addition, such excerpt also fails to even suggest messages, let alone in the specific manner claimed by appellant.

Second, appellant respectfully asserts that the threshold disclosed in Arnold relates to "a [false-positive and false-rejection] probability threshold [that is] used for accepting or rejecting a candidate signature" (see Figure 7, items F and G; Col. 3, lines 41-43; and Col. 10, line 64-Col. 11, line 12). Clearly, determining a threshold for accepting signatures, as set forth in the Arnold excerpt, does not even suggest "content [that] is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value," as claimed by appellant (emphasis added).

Also, with respect to independent Claim 23, the Examiner has relied on Col. 5, lines 21-39; Col., 8, lines 48-57; Col. 9, lines 35-47 and steps 801-823 in Figure 8 of Hitachi to make a prior art showing of appellant's claimed "quarantining the potentially malicious content of the network communications; [and] delivering the network communications over the network upon occurrence of the first of: (i) scanning the potentially malicious content with a malicious code detection file received after the potentially malicious content is received..."

In the latest Office Action dated 12/14/2005, the Examiner has argued that Hitachi discloses "the malicious detection file received after the malicious content see Fig. 8 item 805 and Col 13 Ln 52-Col 14 Ln 19, where the procedure is determined after the quarantine has taken place, i.e. see decision box "data infections?" and that the "Hitachi quarantine(Fig.8 step 804)...takes place before the scanning(Fig. 8 step 805)."

Appellant respectfully asserts that the Hitachi excerpt does not disclose that "the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content." In particular, appellant points out that the Examiner references operation 805 in Figure 8 and Col. 13, lines 52-Col. 14, lines 19 to meet such claim language. Appellant emphasizes, however, that operation 805 in Figure 8 only shows "determin[ing a] download procedure of [the]

file" after "transfer[ing] and quarantin[ing the] file suspected for infection" in operation 804. Thus, Hitachi teaches that only the infected file is downloaded after such infected file is quarantined, and not that "a malicious code detection file [is] received after the potentially malicious content," as claimed by appellant (emphasis added).

To further clarify such distinction, appellant points out that Hitachi expressly discloses that "[i]n step 805, the security agent 651 again notifies to the virus buster 650 in advance a procedure of moving the file 613 transferred in step 803 onto the hard disk 612" where such file 613 is the "file 613 suspected for infection with a computer virus of a new type" (see Col. 13, lines 35-51). Clearly, the Hitachi excerpt teaches that the same file is quarantined and then downloaded, which cannot meet appellant's claim language of a different file, namely the "malicious code detection file" that is "received after the potentially malicious content," as specifically claimed by appellant.

Still with respect to independent Claim 23, the Examiner has relied on Col. 9, lines 18-30 in Hitachi to make a prior art showing of appellant's claimed "cleaning the potentially malicious content if malicious code is found, which is disabling of malicious code." Appellant respectfully asserts that such excerpt only discloses "mov[ing the security software] to the lower-most position on the activation list" and "delet[ing] the software." Clearly, moving and deleting security software, where such software is used for security purposes, as disclosed in the Hitachi excerpt (also see Abstract), does not even suggest "cleaning the potentially malicious," as claimed by appellant.

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 3:

The Examiner has rejected Claim 25 under 35 U.S.C. 103(a) as being unpatentable over Hitachi, Ltd (EP 0893769 A1), in view of Arnold et al. (U.S. Patent No. 5,440,723).

Group #1: Claim 25

The Examiner has relied on paragraph [0024] in Leppek to make a prior art showing of appellant's claimed technique "wherein the heuristics include generating a histogram of content that has been sent over the network during a period of time and analyzing the histogram to determine whether a number of copies of the potentially malicious content that have been sent over the network during the period of time exceed a predetermined value." Appellant respectfully asserts that the histogram in the Leppek excerpt only teaches policy rules for network access control, and does not even suggest "determine[ing] whether a number of copies of the potentially malicious content that have been sent over the network during the period of time exceed a predetermined value," as appellant claims.

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications;

(d) executing a pattern for testing the potentially malicious content network communications for malicious code; and

(e) conditionally delivering the network communications over the network based on the testing;

wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

2. (Original) The method as recited in claim 1, further comprising scanning the network communications for known malicious content.

3. (Original) The method as recited in claim 1, wherein the malicious content includes a mass-mailer virus.

4. (Original) The method as recited in claim 1, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

5. (Original) The method as recited in claim 1, wherein the network communications include electronic mail messages.

6. (Original) The method as recited in claim 5, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

7. (Cancelled)

8. (Previously Presented) The method as recited in claim 1, further comprising cleaning the potentially malicious content if malicious code is found, which is disabling of malicious code.

9. (Previously Presented) A computer program product embodied on a computer readable medium for network-based scanning for potentially malicious content, comprising:

(a) computer code that monitors network communications over a network;

(b) computer code that identifies potentially malicious content in the network communications;

(c) computer code that quarantines the potentially malicious content of the network communications;

(d) computer code that executes a pattern for testing the potentially malicious content network communications for malicious code; and

(e) computer code that conditionally delivers the network communications over the network based on the testing;

wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

10. (Previously Presented) A system for network-based scanning for potentially malicious content, comprising:

(a) logic that monitors network communications over a network;

(b) logic that identifies potentially malicious content in the network communications;

(c) logic that quarantines the potentially malicious content of the network communications;

(d) logic that executes a pattern for testing the potentially malicious content network communications for malicious code; and

(e) logic that conditionally delivers the network communications over the network based on the testing;

wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

11. (Previously Presented) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications; and

(d) delivering the network communications over the network after a predetermined delay;

wherein the delay is for allowing quarantining of the potentially malicious content until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

12. (Original) The method as recited in claim 11, further comprising scanning the network communications for known malicious content.

13. (Original) The method as recited in claim 11, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

14. (Original) The method as recited in claim 11, wherein the network communications include electronic mail messages.

15. (Original) The method as recited in claim 14, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

16. (Cancelled)

17. (Previously Presented) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring network communications over a network;

(b) identifying potentially malicious content in the network communications;

(c) quarantining the potentially malicious content of the network communications in a quarantine; and

(d) delivering the network communications from the quarantine over the network in response to a request from a user;

wherein it is determined whether the user is authorized, and the network communications are delivered only if the user is determined to be authorized;

wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with a malicious code detection file received after the potentially malicious content.

18. (Original) The method as recited in claim 17, wherein the user is an intended recipient of the quarantined network communications.

19. (Cancelled)

20. (Original) The method as recited in claim 17, wherein content is identified as potentially malicious when a number of instances of the content in the network communications is greater than a predetermined value.

21. (Original) The method as recited in claim 17, wherein the network communications include electronic mail messages.

22. (Original) The method as recited in claim 21, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line is greater than a predetermined value.

23. (Previously Presented) A method for network-based scanning for potentially malicious content, comprising:

(a) monitoring incoming and outgoing network communications over a network at a gateway;

(b) scanning the network communications for known malicious content;

(c) identifying potentially malicious content in the network communications;

(d) wherein content is identified as potentially malicious when a number of identical instances of the content in the network communications passing through the network for a given period of time is greater than a predetermined value;

(e) wherein the network communications include electronic mail messages, wherein an electronic mail message is identified as having potentially malicious content when a number of messages having an identical subject line passing through the network for a given period of time is greater than a predetermined value;

(f) quarantining the potentially malicious content of the network communications;

(g) delivering the network communications over the network upon occurrence of the first of:

(i) scanning the potentially malicious content with a malicious code detection file received after the potentially malicious content is received;

(ii) upon receiving a user request;

(iii) upon passage of a predetermined amount of time;

(h) notifying an intended recipient of the potentially malicious content that the potentially malicious content has been quarantined;

(i) notifying a sender of the potentially malicious content that the potentially malicious content has been quarantined; and

(j) cleaning the potentially malicious content if malicious code is found, which is[for] disabling [the]of malicious code.

24. (Previously Presented) The method as recited in claim 1, wherein the potentially malicious content is identified utilizing heuristics.

25. (Previously Presented) The method as recited in claim 24, wherein the heuristics include generating a histogram of content that has been sent over the network during a period of time and analyzing the histogram to determine whether a number of copies of the potentially malicious content that have been sent over the network during the period of time exceed a predetermined value.

26. (Previously Presented) The method as recited in claim 1, wherein the quarantining includes containing the potentially malicious content and preventing the potentially malicious content from creating damage.

27. (Previously Presented) The method as recited in claim 1, wherein when multiple recipients are to receive a copy of the potentially malicious content over the network, a single copy of the potentially malicious content is quarantined and each of the recipients is placed in a list such that after the potentially malicious content is determined to be clean based on the testing, the single copy is forwarded to each of the recipients.

28. (Previously Presented) The method as recited in claim 1, wherein an intended recipient of the network communications is notified that the potentially malicious content is quarantined.

29. (Previously Presented) The method as recited in claim 1, wherein the potentially malicious content is quarantined until the potentially malicious content has been scanned with the malicious code detection file received after the potentially malicious content and after the potentially malicious content is quarantined.

30. (Previously Presented) The method of claim 1, wherein the malicious code detection file is created after the potentially malicious content is identified such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content.

31. (Previously Presented) The method of claim 1, wherein the malicious code detection file is created after the potentially malicious content is received such that a latest malicious code detection file is utilized in the scanning of the potentially malicious content.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY THE APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

There is no such related proceeding.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P040/01.254.01).

Respectfully submitted,

By: _____ Date: 4/17/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660